

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[CUBE Configuration](#)

[CUCM Configuration](#)

[Verify](#)

[Troubleshoot](#)

[Related Cisco Support Community Discussions](#)

Introduction

This document describes the basics of Session Initiation Protocol (SIP) Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) over Cisco Unified Border Element (CUBE) with a configuration example.

Secure voice communication over CUBE can be divided into two parts:

- Secure signaling – CUBE uses TLS to secure signaling over SIP and Internet Protocol Security (IPSec) in order to secure signaling over H.323
- Secure Media – SRTP

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager (CUCM) Certificate Trust List (CTL)
- IP Phones are registered in Secure mode (Encryption)
- CUBE basic voice service voip and dial-peer configuration is done

Components Used

The information in this document is based on these software and hardware versions:

- CUCM 10.5
- CUBE – 3925E with IOS 15.3(3)M3
- Cisco IP Communicator (CIPC)

Background Information

- TLS - TLS and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet.

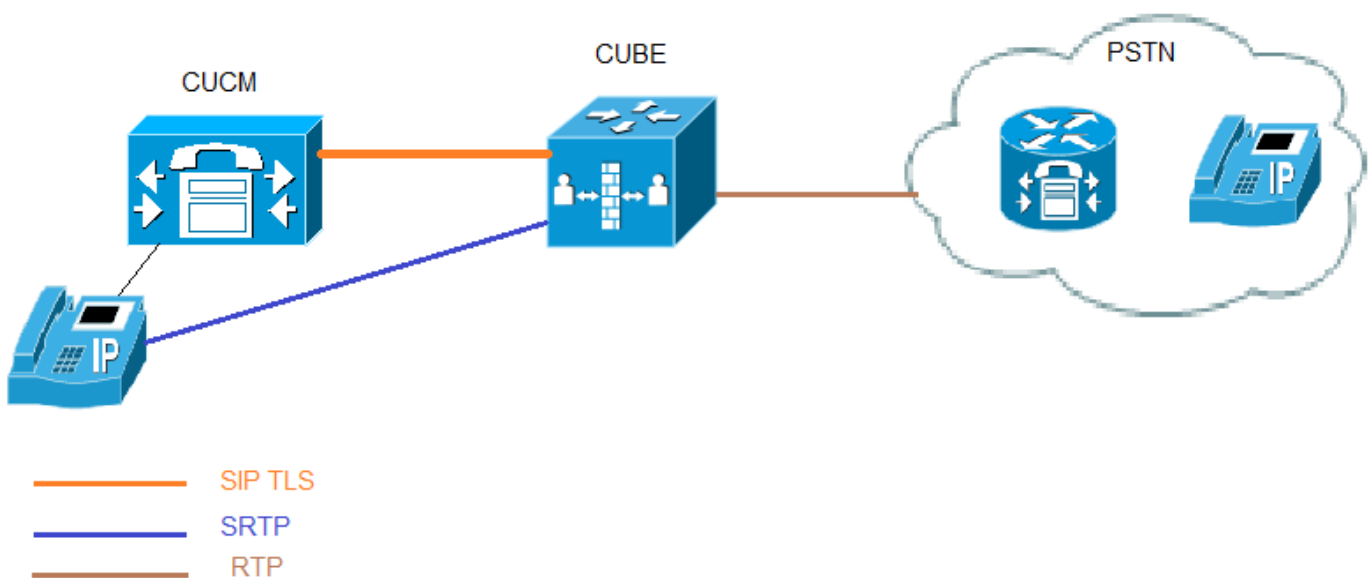
In Open Systems Interconnection (OSI) model equivalences, TLS/SSL is initialized at layer 5 (the session layer) and then works at layer 6 (the presentation layer). In both the models, TLS and SSL work on behalf of the underlying transport layer, whose segments carry encrypted data.

- Certificate Authority (CA) - Trusted entity that issues certificates: Cisco or a third-party entity.
- Device Authentication - Process that validates the identity of the device and ensures that the entity is what it claims to be before a connection is made.
- Encryption - Process of translating data into ciphertext that ensures the confidentiality of the information. Only the intended recipient can read the data. It requires an encryption algorithm and encryption key.
- Public/Private Keys - Keys that are used in encryption. Public keys are widely available, but private keys are held by their respective owners. Asymmetrical encryption combines both types.

Configure

Network Diagram

In this image, the configuration example for setting up SIP TLS and SRTP between CUCM/IP phone and CUBE is shown. CUBE internetworks between SRTP and Real-time Transport Protocol (RTP)



CUBE Configuration

1. Configure clock and enable HTTP server

Synchronize the clocks in the CA server and the client trustpoints (CUBE/OGW/TGW). Otherwise, there are issues with the validity of the certificates issued by the CA server.

Client trustpoints use HTTP to receive certificate from CA.

1. Generate an RSA Keypair

This step generates Private and Public keys.

In this example, CUBE is just a label. It can be anything.

1. Configure IOS CA Server

In this example, CA Server is named cube-ca.

1. Create PKI trustpoints for cube for TLS communication.

In this example, trustpoint name for CUBE is CUBE-TLS. IP address used in enrollment url must be local interface on CUBE. Subject name used in this step must match on X.509 Subject Name on CUCM SIP Trunk security profile. The best practice is to use host-name with domain name (if domain name is enabled).

Associate RSA key pair created in Step 2.

5. Authenticate the trustpoint with CA server and accept certificate of CA.

```
Secure-CUBE(config)#crypto pki authenticate CUBE-TLS
```

Certificate has the following attributes:

```
Fingerprint MD5: BCEBB5A1 1AC882F7 24BE476D 06537711
Fingerprint SHA1: CE2FEEA5 42515B33 3EF6A8F6 7E31D6DF 8E32BEB6
```

```
% Do you accept this certificate? [yes/no]: yes
```

```
Trustpoint CA certificate accepted.
```

```
Secure-CUBE(config)#
```

1. Enroll the trustpoint with CA server.

In this step the CUBE receives a signed certificate from CA.

```
Secure-CUBE(config)#crypto pki enroll CUBE-TLS
```

```
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
```

```
Password:
```

```
Re-enter password:
```

```
% The subject name in the certificate will include: CN=Secure-CUBE
% The fully-qualified domain name will not be included in the certificate
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CUBE-TLS' command will show the fingerprint.
```

```
Secure-CUBE(config)#
```

1. Create the trustpoint for the CUCM.

If CallManager group has multiple CM servers, then trustpoint needs to be created for all servers, otherwise failover not works.

```
crypto pki trustpoint cucmpub
enrollment terminal
revocation-check none
```

```
crypto pki trustpoint cucmsub
enrollment terminal
revocation-check none
```

1. Enroll the CUCM certificate to CUBE.

Step 1. Log in to CUCM OS admin.

Step 2. Navigate to **Security > Certificate Management > Find**.



Step 3. Click the **CallManager** certificate, then download and save .PEM file as shown in this image.

Certificate Details for cmpub, CallManager

Regenerate Generate CSR Download .PEM File Download .DER File

Status

Status: Ready

Certificate Settings

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
Version: V3
Serial Number: 6AA0AECEC947BDCAFCC722310EE83224
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=bangalore, ST=karnataka, CN=cmpub, OU=tac, O=cisco, C=IN
Validity From: Sat Feb 07 22:39:22 IST 2015
To: Thu Feb 06 22:39:21 IST 2020
Subject Name: L=bangalore, ST=karnataka, CN=cmpub, OU=tac, O=cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100d2191a26d52904ae14c3b6eb1a27607d5ca4d85251037db19141e76906d2cfcf5dca3
097fff569b7c19b9705de7624ca441617d49e08ee21a5d5cb8f3583a1f6089278b971833b6132dd4c77e
5e81866f2f4386bc16252658e5bf0c37cb844df8a53a7dc034dff225fe7127b0fba88ab96617d01c3026f1
04eea12492a8572250203010001
Extensions: 3 present
]
```

Regenerate Generate CSR **Download .PEM File** Download .DER File

Step 4. Open the file in the notepad and copy the content from BEGIN CERTIFICATE to END CERTIFICATE .

Step 5. Paste this certificate in CUBE as shown.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
```

```
MIICoJCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBJ
MQswCQYDVQQGEWJUTjEOMAwGA1UEChMFY21zY28xMDEwMDEwMDEwMDEwMDEwMDEw
A1UEAxMFY21zY28xMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEw
b3JlMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEw
SU4xMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEw
MRIwEAYDVQQQIEwlrYXJlYXRha2ExEjAQBgNVBACgYDZDQWw0Y21zY28xMDEwMDEw
hkiG9w0BAQEFAAOBjQAwwYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbS289dyjCX/ /Vpt8GblwXediTKRBYX1J4I7iG11cuPNYOh9giSeLlxgztHt1M
d+XoGGby9DhrwWJSZY5b8MN8uETf1lOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaXMFUwCwYDVR0PBAQDAgK8MCCGA1UdJQQgMB4GCCsGAQUFBwMB
```

```
BggrBgEFBQCDAgYIKwYBBQUHAWUwHQYDVR0OBYYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIB3DQEBAQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBftBoRpKvqRjFt6eIHEtn7+uUIcumDASp
SkX08/Ar
```

-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#

Step 6. Follow same procedure for the other CUCM servers.

1. Configure TCP TLS as transport protocol.

This can be done either at a global or at a dial-peer level.

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIICojCCAagugAwIBAgIQaqCuzs1Hvcr8xyIxDuqyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEWJUTjEOMAWGA1UEChMFY2l2Y28xDDAKBgNVBASATA3RhYzEOMAwG
A1UEAxMFY2l2dWIxZjAQBGNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyM1oXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBGNVBAoTBWNPc2NvMQwwCgYDVQQLEwN0YWMxMDjAMBGNVBAMTBWNTcHVh
MRIWEAYDVQQQIEwlrYXJuYXRha2ExEjAQBGNVBACTCWJhbmhmdhbg9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwYgKcGyEAOhkaJtUpBK4Uw7brGidgfVyK2FJRA32xkUHN
aQbS89dyjCX//Vpt8GblwXediTKRBYX1J4I7iG1lcuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIQ5ZhfQHDAm8QTuoS
SSqFciUCAwEAAAnXMFUwCwYDVROpBAQDAGK8MCcGA1UdJQogMB4GCCsGAQUFBwMB
BggrBgEFBQCDAgYIKwYBBQUHAWUwHQYDVR0OBYYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIB3DQEBAQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBftBoRpKvqRjFt6eIHEtn7+uUIcumDASp
SkX08/Ar
-----END CERTIFICATE-----
```

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#

1. Assign trustpoint for sip-ua, this trustpoint is used for all SIP signaling between CUBE and CUCM

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIICojCCAagugAwIBAgIQaqCuzs1Hvcr8xyIxDuqyJDANBgkqhkiG9w0BAQUFADBj
```

```
MQswCQYDVQGEwJjTjEOMAwGA1UEChMFY2lZy28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2lwdWIxXjAQBGNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMjYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0xDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLLEwN0YWMxDjAMBGNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBGNVBACTCWJhbmhG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKCGyEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHN
aQbS89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG11cuPNYOh9giSeLlxgztHt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQgqMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIB3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
```

-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

or default trustpoint can be configured for all SIP signaling from CUBE.

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

```
MIICoJCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQGEwJjTjEOMAwGA1UEChMFY2lZy28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2lwdWIxXjAQBGNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMjYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0xDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLLEwN0YWMxDjAMBGNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBGNVBACTCWJhbmhG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKCGyEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHN
aQbS89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG11cuPNYOh9giSeLlxgztHt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQgqMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIB3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
```

-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

1. Enable SRTP.

Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIICojCCAagugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJlTjEOMAwGA1UEChMFY2l2Y28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2l2dWIxXjEjAQBGNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0XDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBGNVBAMTBWNTcHVi
MRIwEAYDVQQQIEwlrYXJlYXRha2ExEjAQBGNVBACTCWJhbmhG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKCGYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbS89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG11cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCCGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIB3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsA7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
-----END CERTIFICATE-----
```

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#

1. For SRTP and RTP internetworking, secure transcoder is required.

If IOS version is 15.2.2T (CUBE 9.0) or later then, LTI transcoder can be configure to minimize the configuration.

LTI transcoder doesn't need PKI trustpoint configuration for SRTP-RTP calls

Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIICojCCAagugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJlTjEOMAwGA1UEChMFY2l2Y28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2l2dWIxXjEjAQBGNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0XDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBGNVBAMTBWNTcHVi
MRIwEAYDVQQQIEwlrYXJlYXRha2ExEjAQBGNVBACTCWJhbmhG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKCGYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbS89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG11cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCCGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIB3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsA7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
-----END CERTIFICATE-----
```

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
Secure-CUBE(config)#
If IOS is below 15.2.2T, then configure sccp transcoder.
```

Skinny Call Control Protocol (SCCP) transcoder would need trustpoint for signaling however if same router is used to host the transcoder then same trustpoint(CUBE-TLS) can be used for CUBE as well as transcoder.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIICoJCCAgugAwIBAgIQaqCuzslHvcr8xyIxDuDgyJDANBgkqhkiG9w0BAQUFAADBj
MQswCQYDVQQGEwJtjEOMAwGA1UEChMFY21zY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxExEjAQBGNVBAgTCWthcm5hdGFrYTESMBAGAlUEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0XDTE1MDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBGNVBAOTBWNpc2NvMQwwCgYDVQQLLEwN0YWMxDjAMBGNVBAMTBWNTcHVi
MRIWEAYDVQQIEWlrYXJuYXRha2ExEjAQBGNVBAcTCWJhbmdbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGykCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbS89dyjCX//Vpt8GblwXediTKRBYX1J4I7iG11cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCCGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDgq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMSa7Nk6QmpP5zXKJJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicuDASp
SkXO8/Ar
-----END CERTIFICATE-----
```

```
Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01
```

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
Secure-CUBE(config)#
```

CUCM Configuration

1. Export CUBE IOS certificate to CUCM.

Step 1. Export IOS certificate. Copy self-signed CA certificate and save as .PEM file for example, Secure-CUBE.pem

```
Secure-CUBE(config)#crypto pki export CUBE-TLS pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB/TCCA WagAwIBAgIBATANBgkqhkiG9w0BAQQFADASMRawDgYDVQQDEwdjdWJl
LWNhMB4XDTE1MDIwNzE3MDkyMl0XDTE1MDIwNjE3MDkyMVowEjEQMA4GA1UEAxMH
Y3ViZS1jYTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGykCgYEAtn3gRiUQ409jECyo
xVZzrpBRqj/HOqkVu3iRYp2C2PGRr01vbZvb6IZIh+m4K0Du7gBASUFDAOeidJIF
TCI3+MjUN3grnv1MH32lJ5tVzAPHj9z7GdD42+gZSoHqOM1FB8z4+VDPzpoXpswI
3TFQHCFNbadF16P5VEFWv+0tHD8CAwEAAANjMGEwDwYDVR0TAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAUnqzvazK/7qXzhkoTiAEFCvsN8rww
HQYDVR0OBBYEFJ6s72syv+6184ZKE4gBBQr7DfK8MA0GCSqGSIb3DQEBBAUAA4GB
AEfnNrB4nls81vz0cqlpuTjID+KVyKRwYNP04zJYWCv7P+m1bpMfC/qh14z5/RzL
e5Bq6NUnxWByLR4gcFjmdS1E6NqoNX9S5ryS3xQRkXr0MiXnVngSKELUn22JUw/q
```



```
CEnHng0AvcTRv/EBB2XlzYUxG0keiT8K+jv/g7+rmkF5
-----END CERTIFICATE-----
```

% General Purpose Certificate:

-----BEGIN CERTIFICATE-----

```
MIIB7TCCA VagAwIBAgIBAJANBgkqhkiG9w0BAQUFADASMRAwDgYDVQQDEwdjWJ1
LWNhMB4XDTE1MDIxMTEzMDI1MFoXDTE4MDIxMDEyNTYyMVowFjEUMBIGA1UEAxML
U2VjdXJlLUNVQkUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5C2JnKwtfO
F9bBVYhVwQK8y2c5NMkJCY//pisg+oforvxa1PKAXj/jqDkqtDTc3NAMf2A1rk25
f50aaBrNJmq4rfJB1wLyD2a/CzybJg+QB5sVCCHTwk5jf9+YGIMVsivbrf4m+Lqi
OkZ5qxsMa5fEc/fejUsAE8yn4/mmgld/AgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAF
BgNVHSMEGDAwBSerO9rMr/upfOGShOIAQUK+w3yvDAdBgNVHQ4EFgQUsvUGSpaH
+XIOWvf50imcCHV8HjAwDQYJKoZIhvcNAQEFBQADgYEAYmRHLHxTgIogZYPScPmj
h69GLxXxAOTHhOsEbm/vfqk2vbYiHU09AtDDI+kNecSuOGmd7fokJMP9K1xc1i2a
vrr2qwQYqRAh68BwTjWzR3mFAGbDZzWiywv1jJ92ra3EMAUc0sJZSLzGY0+BjO/E
dEW6JUIOx3Nxp2SBN1NMAQ0=
```

-----END CERTIFICATE-----

Secure-CUBE(config)#

Step 2. Upload IOS CA certificate on CUCM as CallManager-trust.

Step 3. Navigate to **CM OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain**

Step 4. Upload .PEM file as shown in this image.

Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* **CallManager-trust**

Description(friendly name)

Upload File **Browse...** Secure-CUBE.pem

Upload Close

i *- indicates required item.

1. Create New SIP Trunk Security Profile

Step 1. On CM Administration navigate to **System > Security > SIP Trunk Security Profiles > File**.

Step 2. Copy the existing **Non Secure SIP Trunk Profile** in order to create new secure profile as

shown in this image.

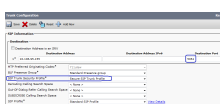
The screenshot shows the 'SIP Trunk Security Profile Configuration' page. The 'Device Security Mode' is set to 'Encrypted' and the 'X.509 Subject Name' is set to 'Secure-CUBE'. Other visible settings include: Name: Secure SIP Trunk Profile; Description: Secure SIP Trunk Profile authenticated by null String; Incoming Transport Type: TLS; Outgoing Transport Type: TLS; Nonce Validity Time (mins): 600; Incoming Port: 5061. Several checkboxes are checked, including 'Accept presence subscription', 'Accept out-of-dialog refer**', 'Accept unsolicited notification', and 'Accept replaces header'.

1. Create SIP trunk to the CUBE

Step 1. Enable SRTP on SIP trunk as shown in this image.

The screenshot shows the 'Trunk Configuration' page. The 'SRTP Allowed' checkbox is checked and highlighted with a blue box. The 'Consider Traffic on This Trunk Secure*' dropdown is set to 'When using both sRTP and TLS'. Other visible settings include: Packet Capture Mode: None; Packet Capture Duration: 0; 'Retry Video Call as Audio' is checked; 'PSTN Access' and 'Run On All Active Unified CM Nodes' are checked.

Step 2. Configure Destination Port 5061 (TLS) and apply New Secure SIP trunk Security profile on the SIP trunk as shown in this image.



Verify

```
Secure-CUBE#show sip-ua connections tcp tls detail
```

```
Total active connections : 2
```

```
No. of send failures : 0
```

```
No. of remote closures : 13
```

```
No. of conn. failures : 0
```

```
No. of inactive conn. ageouts : 0
```

```
TLS client handshake failures : 0
```

```
TLS server handshake failures : 0
```

```
-----Printing Detailed Connection Report-----
```

```
Note:
```

```
** Tuples with no matching socket entry
```

```
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
```

```
to overcome this error condition
```

```
++ Tuples with mismatched address/port entry
```

```
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
```

```
to overcome this error condition
```

```
Remote-Agent:10.106.95.151, Connections-Count:2
```

```
Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
```

```
=====
```

```
5061 16 Established 0 10.106.95.155
```

```
57396 17 Established 0 10.106.95.155
```

```
----- SIP Transport Layer Listen Sockets -----
```

```
Conn-Id Local-Address
```

```
=====
```

```
2 [10.106.95.155]:5061
```

Output of show call active voice brief is captured when LTI transcoder is used.

```
Secure-CUBE#show call active voice brief
```

```
Telephony call-legs: 0
```

```
SIP call-legs: 2
```

```
H323 call-legs: 0
```

```
Call agent controlled call-legs: 0
```

```
SCCP call-legs: 0
```

```
Multicast call-legs: 0
```

```
Total call-legs: 2
```

```
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
```

```
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
```

```
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
```

```
off Transcoded: Yes
```

```
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
```

```
long duration call detected:n long duration call duration:n/a timestamp:n/a
```

```
LostPacketRate:0.00 OutOfOrderRate:0.00
```

```
1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
```

```
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
```

```
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
```

```
Transcoded: Yes
```

```
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
```

```
long duration call detected:n long duration call duration:n/a timestamp:n/a
```

```
LostPacketRate:0.00 OutOfOrderRate:0.00
```

Also when an SRTP encrypted call is made between Cisco IP phone and CUBE or Gateway, a lock icon is displayed on the IP phone.

Troubleshoot

These debugs are helpful for troubleshooting PKI/TLS/SIP/SRTP issues.

```
Secure-CUBE#show call active voice brief
```

```
Telephony call-legs: 0
```

```
SIP call-legs: 2
```

```
H323 call-legs: 0
```

```
Call agent controlled call-legs: 0
```

```
SCCP call-legs: 0
```

```
Multicast call-legs: 0
```

```
Total call-legs: 2
```

```
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
```

```
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
```

```
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
```

```
off Transcoded: Yes
```

```
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
```

```
long duration call detected:n long duration call duration:n/a timestamp:n/a
```

```
LostPacketRate:0.00 OutOfOrderRate:0.00
```

```
1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
```

```
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
```

```
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
```

```
Transcoded: Yes
```

```
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
```

```
long duration call detected:n long duration call duration:n/a timestamp:n/a
```

```
LostPacketRate:0.00 OutOfOrderRate:0.00
```